Amendments to the Claims:

This Listing of the Claims replaces all prior versions, and listings, of the Claims in this Application.

Listing of Claims:

1. (presently amended) A method for encrypting and decrypting data comprising ~~steps of~~:

generating a random number sequence;

transmitting the random number sequence to a data encryption station and a data decryption station;

generating a private key;

inputting the private key to the data encryption station and to the data decryption station;

selecting at the data encryption station an encryption subsequence from the random number sequence, the boundaries of the encryption subsequence based on the private key;

encrypting a plaintext data at the data encryption station based on the private key and the selected encryption subsequence and generating, as a result, an encrypted data;

transmitting the encrypted data from the encryption station to the decryption station;

selecting at the data decryption station, based on the private key input to the decryption station, a decryption subsequence from the random number sequence, the boundaries of the decryption subsequence being identical to the boundaries of the encryption subsequence; and

decrypting the encrypted data at the data decryption station based on the private key and selection decryption sequence and generating, as a result, a recovered plaintext data.

2. (presently amended) A method according to claim 1 further comprising ~~steps of~~:

generating a synchronization signal;

generating, at the encryption station, a first sampling time t based on the input private key;

sampling the random number sequence at the encryption station for a predetermined interval beginning at a time based on t, to generate a sampled block of bits; and

storing the sampled block of bits in a random number reservoir,

wherein said encrypting step is based, in part, on a content of said random number reservoir.

3. (presently amended) A method according to claim 1, further comprising ~~steps of~~:

generating a synchronization signal;

generating, at the encryption station, a sampling time t based on the input private key;

sampling the random number sequence at the encryption station for a predetermined interval beginning at a time based on t, to generate a sampled block of bits;

detecting a number of bits in said random number reservoir;

comparing the number of bits detected by said detecting step with a predetermined reservoir full value; and

based on said comparing ~~step~~ detecting the number of bits in said random number reservoir being less than said predetermined reservoir full value, performing a step of storing the sampled block of bits in a random number reservoir,

wherein said encrypting step is based, in part, on a content of said random number reservoir.

4. (presently amended) A method according to claim 3 further comprising ~~steps of~~:

based on said comparing ~~step~~ detecting the number of bits in said random number reservoir being less than said predetermined reservoir full value, performing ~~steps of~~:

(a) generating a new private key based on the sampled block of bits and the previous private key;

(b) generating a new sampling time t based, at least in part, on the new private key;

(c) sampling an additional block of bits from the random number sequence, at a sampling time based on the new sampling time t;

(d) detecting a number of bits in said random number reservoir;

(e) comparing the number of bits detected by said detecting step with a predetermined reservoir full value;

(f) based on said comparing ~~step~~ detecting the number of bits in said random number reservoir being less than said predetermined reservoir full value, performing a step of storing the sampled additional block of bits in said random number reservoir; and

(g) repeating ~~steps~~ (a) through (f) until said comparing ~~step~~ detects the number of bits in said random number reservoir as being greater than or equal to said predetermined reservoir full value.

5. (presently amended) A method according to claim 1 wherein said ~~step of~~ transmitting the random number sequence includes ~~steps of~~:

transmitting said random number sequence by uplink up to a satellite;

transmitting said random number sequence received by said satellite down to said encryption station and to said decryption station.

6. (new) A method for encrypting data comprising:

broadcasting a random symbol sequence;

broadcasting a synchronization signal;

generating a private key;

providing said private key to an encryption station and to a decryption station;

receiving said random number sequence at said encryption station and said decryption station;

receiving said synchronization signal at said encryption station and at said decryption station;

selecting an encrypting subsequence from said random number sequence received at said encryption station, said selection based on said synchronization signal received at said encryption station and on said private key;

providing a message symbol sequence to said encryption station;

encrypting said message symbol sequence, at said encryption station, based on said encrypting subsequence, into an encrypted symbol sequence.

7. (new) A method for encrypting data according to claim 6, further comprising:

transmitting said encrypted symbol sequence from said encryption station to said decryption station;

selecting at the decryption station a decryption subsequence from the random number sequence, the boundaries of said decryption subsequence based on the private key, the selection being such that the decryption subsequence is identical to said encryption subsequence;

decrypting said encrypted symbol sequence, at said decryption station, based on said decrypting subsequence, into said message symbol sequence.